Quelle: TensorSpark – stock.adobe.com

IEC 62443 und ISO 27001

Cybersicherheit für Industrie und Gewerbe (1)

Stellen Sie sich vor, Ihr Zuhause ist Ihre digitale Welt. Die Tür Ihres Hauses entspricht der Firewall Ihres Computers, die Fenster den einzelnen Programmen und Apps, die Sie nutzen, und Ihre persönlichen Gegenstände den sensiblen Daten, die Sie aufbewahren. Genau wie Sie Ihr Zuhause vor Einbrechern schützen möchten, müssen Sie auch Ihre digitale Welt vor Cyberkriminellen schützen.

Die gute Nachricht ist: Die grundlegenden Prinzipien der Sicherheit sind sowohl in der realen Welt als auch im Cyberspace gleich. Einen groben Überblick zu den Inhalten des gesamten Artikels bietet die Grafik in **Bild 1**.

Parallelen aus dem Alltag

Lassen Sie uns einige Parallelen zwischen Cybersicherheit und dem Alltag aufzeigen, die Ihnen die abstrakten Konzepte der digitalen Sicherheit näherbringen (vgl. Kasten »**Cybersecurity im privaten Umfeld**«):

- **Abschließen und Sichern**: So wie Sie Ihre Haustür und Fenster nachts abschließen, sollten Sie auch Ihre Passwörter stark und geheim halten und sicherstellen, dass Ihre Geräte mit einem Virenscanner und einer Firewall geschützt sind.
- **Vorsicht bei Fremden**: Seien Sie im Internet genauso vorsichtig wie im realen Leben. Öffnen Sie keine E-Mails oder Anhänge von unbekannten Absendern, klicken Sie nicht auf verdächtige Links und geben Sie persönliche Daten nur auf seriösen Websites ein.
- **Wertgegenstände schützen**: Bewahren Sie Ihre wertvollsten Gegenstände, wie z. B. Schmuck oder Bargeld, in einem Safe auf. Ebenso sollten Sie Ihre sensiblen Daten, wie z. B. Bankkontoinformationen oder Passwörter, verschlüsseln und an einem sicheren Ort aufbewahren.

Quelle: M. Wiener

Bild 1: *Übersicht zu den Themen des gesamten Beitrags*

- **Auf dem Laufenden bleiben**: Informieren Sie sich über die neuesten Bedrohungen und Sicherheitslücken, genau wie Sie sich über die neuesten Einbruchstechniken informieren würden. Installieren Sie regelmäßig Sicherheitsupdates für Ihre Software und Betriebssysteme.
- **Vertrauen Sie Ihrem Instinkt**: Wenn Ihnen etwas im Internet verdächtig vorkommt, ist es wahrscheinlich auch so. Seien Sie vorsichtig und gehen Sie kein Risiko ein.

Indem Sie diese einfachen Parallelen zwischen Cybersicherheit und dem Alltag beherzigen, können Sie Ihre digitale Welt deutlich sicherer gestalten und sich vor Cyberangriffen schützen. So viel zu uns und unserem größtenteils privaten Alltag, denn dieser Abschnitt sollte in erster Linie das Bewusstsein für das Thema schärfen. Im Weiteren klären wir zunächst einige grundlegende Fragen und richten den Fokus später auf die Industrie.

Cybersicherheit in der digitalen Welt

In der heutigen Zeit, die von der Vernetzung und Digitalisierung geprägt ist, spielt Cybersicherheit eine zentrale Rolle für den Schutz von Individuen, Unternehmen und ganzen Nationen. Die rasante Entwicklung neuer Technologien und die zunehmende Abhängigkeit von digitalen Infrastrukturen schaffen jedoch auch neue Herausforderungen und Bedrohungen (**Bild 2**).

Was ist Cybersicherheit?

Cybersicherheit umfasst alle Maßnahmen, die darauf abzielen, Systeme, Netzwerke und Daten vor unbefugtem Zugriff, Nutzung, Offenlegung, Änderung oder Zerstörung zu schützen. Sie ist ein komplexes Thema, das verschiedene Bereiche wie IT-Sicherheit, Informationssicherheit, Datensicherheit und Netzwerksicherheit einschließt.

Warum ist Cybersicherheit wichtig?

Die Bedrohungen durch Cyberkriminalität nehmen stetig zu. Hacker, Spione und andere Cyberkriminelle entwickeln ständig neue Methoden, um an sensible Daten zu gelangen, Systeme zu sabotieren oder finanzielle Vorteile zu erzielen. Die Folgen eines Cyberangriffs können für Unternehmen und Privatpersonen immens sein:

- **Finanzieller Schaden**: Durch Diebstahl von Kreditkartendaten, Lösegeldforderungen oder Betriebsunterbrechungen.
- **Reputationsverlust**: Durch Datenlecks, Identitätsdiebstahl oder öffentliche Bloßstellung.
- **Betriebsunterbrechungen**: Durch den Ausfall kritischer Systeme.
- **Spionage und Sabotage**: Durch Diebstahl von Geschäftsgeheimnissen oder Sabotage von Industrieanlagen.

Mit diesen Hintergrundinformationen haben wir nun eine grundlegende Basis geschaffen, um den Blick in Richtung der Industrie zu lenken und uns mit den wichtigsten Themen, wie z. B. reibungslose und sichere Produktionsabläufe etc. zu beschäftigen.

Cybersicherheit für die Industrie: Ein Überblick

Die digitale Transformation der Industrie, bekannt als Industrie 4.0, hat die Vernetzung von Maschinen, Anlagen und Produktionsprozessen mit dem Internet vorangetrieben. Dies bringt zwar enorme Effizienzsteigerungen und neue Möglichkeiten, erhöht aber gleichzeitig die Angriffsfläche für Cyberbedrohungen.

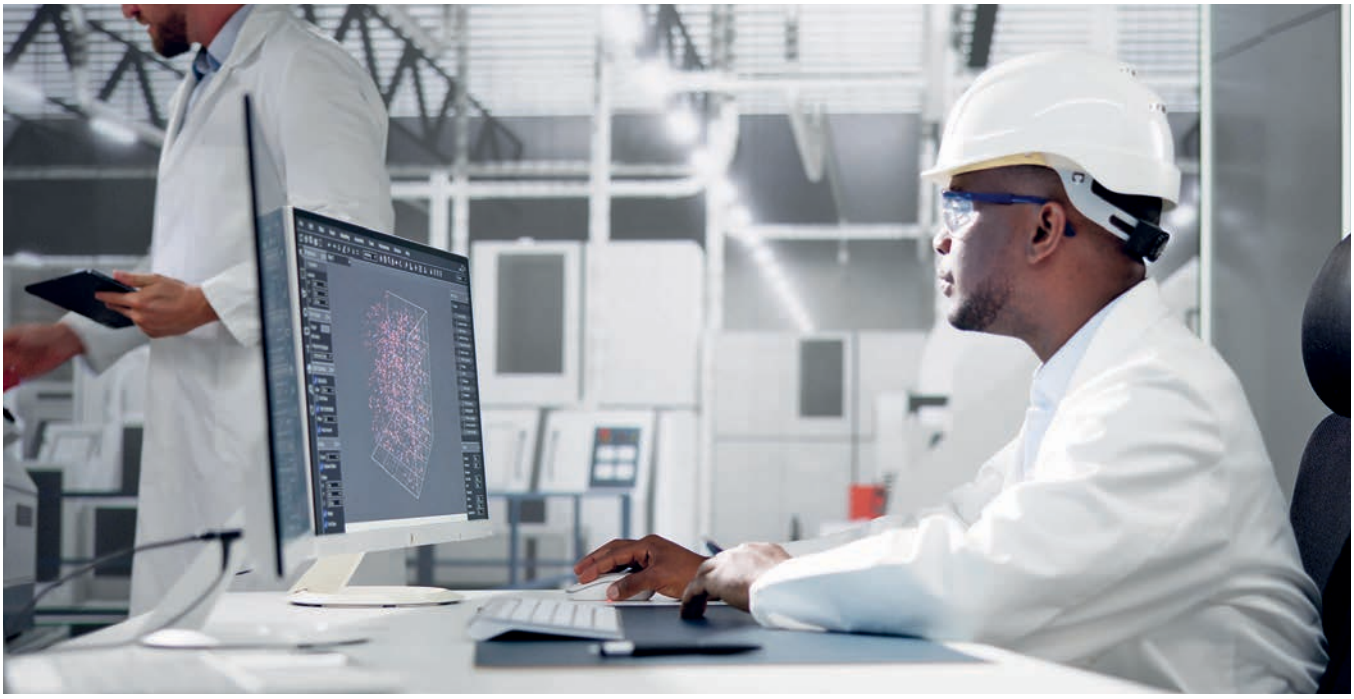
Die folgenden Punkte sind die wichtigsten Themen rund um die Cybersicherheit für die Industrie.

1. Bedrohungen

- **Vermehrte Angriffe auf industrielle Steuerungssysteme** (ICS): Hacker können diese Systeme manipulieren, um die Produktion zu stören, sensible Daten zu stehlen oder sogar physischen Schaden anzurichten.
- **Supply-Chain-Angriffe**: Schadsoftware kann über Lieferanten in die industriellen Systeme gelangen.
- **Ransomware-Angriffe**: Kritische Systeme werden durch Verschlüsselung blockiert, und die Angreifer fordern Lösegeld für die Freigabe.
- **Spionage und Datendiebstahl**: Geschäftsgeheimnisse und Know-how können durch gezielte Angriffe von Konkurrenten oder Hackern entwendet werden.

2. Schutzmaßnahmen

- **Risikobewertung und Schutzbedarfsanalyse**: Identifizierung und Priorisierung von potenziellen Bedrohungen und Schwachstellen.
- **Implementierung eines Zero-Trust-Sicherheitsmodells**: Zugriff nur gewähren, wenn er explizit benötigt und autorisiert wird.
- **Segmentierung von Netzwerken**: Trennung von IT- und OT-Netzwerken sowie kritischen Systemen untereinander.



Quelle: Andrey Popov – stock.adobe.com

Bild 2: *Die Vernetzung von Maschinen, Anlagen und Produktionsprozessen birgt auch die Verbreiterung der Angriffsfläche für Cyberbedrohungen*

- **Härtung von Systemen**: Regelmäßige Updates und Patches, Deaktivierung unnötiger Funktionen und Dienste.
- **Schulung und Bewusstseinsbildung**: Sensibilisierung der Mitarbeiter für Cybersicherheitsrisiken und Verhaltensweisen im Ernstfall.

Cybersecurity für zuhause: So schützen Sie Ihre Daten

Im digitalen Alltag sind wir ständigen Bedrohungen ausgesetzt. Um Ihre Daten zu schützen, sollten Sie folgende Maßnahmen ergreifen:

- **Starke Passwörter**: Verwenden Sie lange, komplexe Kombinationen aus Buchstaben, Zahlen und Sonderzeichen. Zusätzlich können Sie sich durch einen Passwort-Manager die Verwaltung erheblich erleichtern.
- **Zwei-Faktor-Authentifizierung**: Aktivieren Sie diese zusätzliche Sicherheitsebene, um unbefugten Zugriff zu verhindern.
- **Software-Updates**: Halten Sie Ihr Betriebssystem und Programme immer auf dem neuesten Stand.
- **Sichere WLAN-Netzwerke**: Verwenden Sie sichere Passwörter und verschlüsseln Sie Ihr WLAN.
- **Antiviren-Software**: Schützen Sie Ihren Computer mit einer aktuellen Antivirenlösung.

Fazit: Cybersecurity ist kein Einmalprojekt, sondern ein kontinuierlicher Prozess!

3. Normen und Standards

- **IEC 62443**: Internationaler Standard für die Cybersicherheit industrieller Automatisierungssysteme.
- **ISO/IEC 27001**: Internationaler Standard für Informationssicherheitsmanagementsysteme.

Die Bedrohungen machen das Ausmaß und den daraus möglicherweise entstehenden Schaden deutlich. Die Schutzmaßnahmen zeigen, dass Cybersicherheit ein fortlaufender Prozess ist, der in Unternehmen eine hohe Wichtigkeit genießen muss. In diesem Zusammenhang sind die aufgeführten Normen und Standards von hoher Bedeutung, daher werden wir diese nun etwas genauer beleuchten, da diese die essenziellen Grundlagen für den Schutz vor Cyberangriffen in der Industrie darstellen. An dieser Stelle sei angeführt, dass die beiden aufgeführten Normen in meinen Augen die höchste Bedeutung haben und daher hier vertieft werden.

IEC 62443 – Bollwerk gegen Cyberangriffe

Allgemeines

Die Norm IEC 62443 ist ein internationaler Standard, der Sicherheitsanforderungen für industrielle Automatisierungs- und Steuerungssysteme (IACS) festlegt. Diese Norm wurde entwickelt, um sicherzustellen, dass industrielle Netzwerke und Systeme gegen Cyberangriffe geschützt sind und um Sicherheitslücken in diesen Systemen zu minimieren. Die IEC 62443 wurde von der Internationalen Elektrotechnischen Kommission (IEC) entwickelt. Sie richtet sich an verschiedene Stakeholder (Interessensvertreter) in der industriellen Automatisierung, einschließlich Hersteller von Steuerungssystemen, Systemintegratoren und Betreiber von industriellen Anlagen.

Das Hauptziel der Norm ist es, eine robuste Cybersicherheitsbasis für IACS zu schaffen und so die Zuverlässigkeit, Sicherheit und Verfügbarkeit dieser Systeme zu gewährleisten. Die IEC 62443 ist in mehrere Teile gegliedert, die jeweils unterschiedliche Aspekte der Cybersicherheit für IACS abdecken, dazu nachfolgend einige Beispiele.

- **IEC 62443-1-x**: Allgemeine Konzepte: Dieser Teil beinhaltet grundlegende Definitionen, Konzepte und Modelle für die IACS-Sicherheit.
- **IEC 62443-4-x**: Komponentenanforderungen: Der Teil 4 richtet sich an die Anforderungen auf Komponentenebene, einschließlich individueller Geräte und Steuerungen.

Vorteile

Durch die Umsetzung der Norm können Unternehmen die Sicherheit ihrer industriellen Systeme erheblich verbessern und so das Risiko von Cyberangriffen reduzieren. Viele Branchen, insbesondere kritische Infrastrukturen wie Energie, Wasser und Transport,

verlangen die Einhaltung strenger Sicherheitsstandards.

Die Einhaltung der IEC 62443 kann das Vertrauen in die Sicherheit und Zuverlässigkeit der Systeme erhöhen. Unternehmen, die die Norm erfüllen, können sich auf dem Markt als sicherheitsbewusst positionieren und sich so einen Wettbewerbsvorteil verschaffen. In vielen Ländern gibt es zunehmend gesetzliche und regulatorische Anforderungen an die Cybersicherheit industrieller Systeme. Die IEC 62443 bietet eine umfassende Grundlage zur Erfüllung dieser Anforderungen.

Die Norm ist somit ein wichtiger Standard für die Cybersicherheit industrieller Automatisierungs- und Steuerungssysteme. Sie bietet eine strukturierte und umfassende Herangehensweise an die Sicherung dieser Systeme und ist für die Industrie von großer Bedeutung, um die Zuverlässigkeit, Sicherheit und Verfügbarkeit von IACS zu gewährleisten. Trotz der Herausforderungen bei der Umsetzung bietet sie erhebliche Vorteile hinsichtlich der Risikominderung und der Einhaltung gesetzlicher und regulatorischer Anforderungen.

ISO 27001: Ein Leitfaden zum Schutz Ihrer Informationen

Die Norm ISO/IEC 27001 ist ein international anerkannter Standard für das Management der Informationssicherheit (**Bild 3**). Er definiert Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems (ISMS).

Die ISO/IEC 27001 wurde von der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) entwickelt. Sie zielt darauf ab, den Schutz vertraulicher Daten zu gewährleisten, die Integrität und Verfügbarkeit von Informationen sicherzustellen und das Risiko von Sicherheitsvorfällen zu minimieren. Die ISO/IEC 27001 ist strukturiert, um systematisch die Anforderungen an ein ISMS zu definieren. Sie gliedert sich in mehrere Abschnitte:

- Einführung und Anwendungsbereich
- Normative Verweisungen
- Begriffe und Definitionen
- Kontext der Organisation
- Führung
- Planung
- Unterstützung
- Betrieb

Quelle: Pakin – stock.adobe.com

Bild 3: *Die Norm ISO/IEC 27001 ist ein international anerkannter Standard für das Management der Informationssicherheit*

- Bewertung der Leistung
- Verbesserung.

Bedeutung für die Industrie

Die ISO 27001 hat eine große Bedeutung für verschiedene Industrien und bietet zahlreiche Vorteile. So zum Beispiel die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, was besonders wichtig für sensible Daten und geistiges Eigentum ist. Weiterhin die Unterstützung bei der Einhaltung gesetzlicher und regulatorischer Anforderungen bezüglich Datenschutz und Informationssicherheit. Außerdem sind die Demonstration des Engagements für Informationssicherheit gegenüber Kunden, Partnern und anderen Interessengruppen, was das Vertrauen und die Reputation des Unternehmens stärkt, zu nennen. Unternehmen, die nach ISO 27001 zertifiziert sind, können sich auf dem Markt als sicherheitsbewusst positionieren und dadurch einen Wettbewerbsvorteil erlangen.

Auch die Implementierung der ISO 27001 kann mit verschiedenen Herausforderungen verbunden sein. Die Einrichtung und Aufrechterhaltung eines ISMS kann komplex und ressourcenintensiv sein, insbesondere für kleinere Unternehmen. Die Implementierung und Zertifizierung nach ISO 27001 kann mit erheblichen Kosten verbunden sein. Es erfordert eine Kultur der Informationssicherheit im Unternehmen und entsprechende Schulungen für Mitarbeiter, um sicherzustellen, dass Sicherheitsmaßnahmen effektiv umgesetzt werden. Das ISMS erfordert eine kontinuierliche Überprüfung und Verbesserung, was einen fortlaufenden Einsatz von Ressourcen und Engagement seitens der Geschäftsleitung erfordert.

Die ISO/IEC 27001 ist ein essenzieller Standard für die Informationssicherheit, der Unternehmen hilft, ihre Informationen zu schützen und Risiken zu managen. Trotz der Herausforderungen bei der Implementierung bietet die Norm erhebliche Vorteile, darunter erhöhter Schutz sensibler Daten, Erfüllung regulatorischer Anforderungen und Stärkung der Marktposition. Die ISO 27001 trägt dazu bei, Vertrauen und Reputation zu fördern und schafft eine Grundlage für eine systematische und kontinuierliche Verbesserung der Informationssicherheit.

(Fortsetzung folgt)

FÜR SCHNELLLESER

Zeitgemäße Cybersicherheit ist allein schon für Privatpersonen sehr wichtig, für Industrieunternehmen und auch Handwerksbetriebe unabdingbar

Diese Sicherheit beinhaltet verschiedene Kriterien, die im gesamten Beitrag (Teil 1 und 2) eingehend beleuchtet werden

Im Fokus des ersten Teils stehen die Normen IEC 62443 und ISO/IEC 27001

Autor:
Michael Wiener, M. Eng,
Dozent am Fachbereich Elektro- und Informationstechnik der Hochschule Fulda

Quelle: M. Wiener

Bild 1: *Übersicht zu den Themen des zweiten Teils*

Der Cyber Resilliance Act (CRA)

Cybersicherheit für Industrie und Gewerbe (2)

In dieser Ausgabe folgt der zweite Teil zum Thema Cybersicherheit, bei dem wir den Schwerpunkt u. a. auf den Cyber Resilience Act (CRA) legen und dessen Bedeutung für Unternehmen in den Mittelpunkt stellen. Eine Übersicht zu den Inhalten liefert auch **Bild 1**.

Bevor wir tiefer in die Thematik einsteigen, hier noch eine kleine Anknüpfung an das bisher Gesagte: wir betrachteten uns im ersten Teil die Cybersicherheit in der digitalen Welt und stellten uns die Fragen, was der Begriff Cybersicherheit bedeutet und warum Cybersicherheit für alle so wichtig ist. Es folgten eine Gegenüberstellung der wichtigsten Normen und Standards in Form von der IEC 62443 und ISO 27001.

Der Cyber Resilliance Act (CRA) – ein umfassender Überblick

Was ist der CRA?

Der CRA ist ein neues Gesetz der Europäischen Union, das darauf abzielt, die Cybersicherheit in der EU zu stärken und Unternehmen sowie Bürger besser vor Cyberangriffen zu schützen. Er stellt einen Meilenstein in der europäischen Cybersecurity-Strategie dar und soll dazu beitragen, die digitale Widerstandsfähigkeit der EU zu erhöhen. Der CRA ist noch nicht vollständig in Kraft getreten. Es gab jedoch bereits mehrere wichtige Meilensteine:

- ***Einführung in das Europäische Parlament***: Der CRA wurde im September 2022 in das Europäische Parlament eingebracht.
- ***Verabschiedung***: Im März 2024 wurde der CRA vom Europäischen Parlament angenommen.
- ***Inkrafttreten***: Am 20.11.2024 wurde der CRA in einem Amtsblatt der EU veröffentlicht und ist seit 11.12.2024 wirksam (**Bild 2**). Als Hersteller von Produkten, die dem CRA unterliegen, müssen die Anforderungen des Cyber Resilience Acts ab dem 11.12.2027 erfüllt werden.

Hintergrund und Ziele

- ***Steigende Cyberbedrohungen***: Die Zunahme und Komplexität von Cyberangriffen in den letzten Jahren hat gezeigt, dass ein umfassenderer und einheitlicherer Ansatz zur Cybersicherheit in der EU erforderlich ist.
- ***Fragmentierte Landschaft***: Vor dem CRA war die Cybersicherheit in der EU durch eine Vielzahl nationaler Gesetze und Vorschriften gekennzeichnet, was zu einer fragmentierten Landschaft führte.
- ***Schwachstellen in der Lieferkette***: Der CRA zielt auch darauf ab, Schwachstellen in der Lieferkette von Produkten mit digitaler Funktionalität zu schließen.
- ***Höhere Sicherheitsstandards***: Durch die Einführung strengerer Anforderungen an die Sicherheit von Produkten und Dienstleistungen soll ein höherer Sicherheitsstandard in der gesamten EU erreicht werden.
- ***Verbesserte Transparenz***: Unternehmen müssen künftig mehr Informationen über die Sicherheit ihrer Produkte und Dienstleistungen offenlegen.
- ***Stärkere Zusammenarbeit***: Der CRA fördert die Zusammenarbeit zwischen den Mitgliedstaaten und den EU-Institutionen im Bereich der Cybersicherheit.
- ***Reaktion auf Cyberangriffe***: Durch die Einführung von Meldepflichten soll eine schnellere Reaktion auf Cyberangriffe ermöglicht werden.

Kernpunkte des CRA

- ***Anforderungen an Produkte***: Der CRA enthält detaillierte Anforderungen an die Sicherheit von Produkten mit digitaler Funktionalität, wie z. B. Software, IoT-Geräte und industrielle Steuerungssysteme.
- ***Risikobewertung***: Hersteller müssen eine Risikobewertung durchführen, um Schwachstellen in ihren Produkten zu identifizieren und zu beheben.
- ***Sicherheitsupdates***: Unternehmen müssen sicherstellen, dass ihre Produkte regelmäßig mit Sicherheitsupdates versorgt werden.
- ***Meldepflichten***: Hersteller müssen bestimmte Cybervorfälle melden, um eine schnellere Reaktion auf Bedrohungen zu ermöglichen.
- ***Zertifizierung***: Der CRA sieht die Einführung eines europäischen Zertifizierungssystems für Cybersecurity-Produkte vor.

Was bedeutet der CRA für Unternehmen?

Der CRA stellt Unternehmen vor neue Herausforderungen, da sie ihre Produkte und Prozesse an die neuen Anforderungen anpassen müssen. Dies kann erhebliche Investitionen erfordern. Gleichzeitig bietet der CRA auch Chancen, da Unternehmen, die sich frühzeitig an die neuen Regeln anpassen, einen Wettbewerbsvorteil gewinnen können.

Aktiv werden: Was können Betriebe jetzt tun?

Nachfolgend gebe ich einen wesentlichen Überblick, im Abschnitt Praxisbeispiel erfolgt eine ausführliche Betrachtung zu einem möglichen Vorgehen in der Praxis.

- ***Risikoanalyse durchführen***: Unternehmen sollten eine umfassende Risikoanalyse durchführen, um ihre aktuelle Sicherheitslage zu bewerten und Schwachstellen zu identifizieren.
- ***Compliance-Management-System einführen***: Ein solches System hilft Unternehmen, die neuen Anforderungen des CRA umzusetzen und nachzuweisen.
- ***Schulungen für Mitarbeiter***: Mitarbeiter müssen für die Bedeutung von Cybersecurity sensibilisiert werden.
- ***Lieferanten überprüfen***: Unternehmen sollten ihre Lieferanten auf deren Cybersecurity-Praktiken prüfen.
- ***Zertifizierungen anstreben***: Eine Zertifizierung nach den neuen europäischen Standards kann ein Wettbewerbsvorteil sein.

Aber Moment mal, IEC 62443, ISO 27001 und CRA, gibt es hier Verbindungen? Dies betrachten wir ausführlich im nächsten Abschnitt.

Quelle: artjazz – stock.adobe.com

Bild 2: *Mit der Einführung des CRA will die EU eine weitgehende Vereinheitlichung der Cybersicherheitsstandards für die Mitgliedsstaaten erreichen*

Zusammenspiel von CRA, IEC 62443 und ISO 27001

Der CRA bildet einen übergreifenden Rahmen für die Cybersicherheit in der EU. Innerhalb dieses Rahmens spielen die Normen IEC 62443 und ISO 27001 eine entscheidende Rolle, denn sie bieten konkrete technische und organisatorische Maßnahmen zur Umsetzung der im Act formulierten Ziele.

- ***IEC 62443***: Der CRA bezieht sich in vielerlei Hinsicht auf die IEC 62443, die als De-facto-Standard für die Sicherheit von industriellen Automatisierungssystemen gilt. Unternehmen, die in diesem Bereich tätig sind, müssen die Anforderungen der IEC 62443 erfüllen, um dem CRA zu entsprechen.
- ***ISO 27001***: Der CRA bezieht sich ebenfalls auf die ISO 27001, da sie einen etablierten Rahmen für den Aufbau und die kontinuierliche Verbesserung von Informationssicherheit bietet. Unternehmen können die ISO 27001 nutzen, um die im CRA geforderten Anforderungen an die Informationssicherheit umzusetzen.

CRA, IEC 62443 und ISO 27001: Dann ist ja alles klar?!

Leider nein! Denn es gibt kein »Rezept« für Cybersicherheit. Weder der CRA noch Normen wie IEC 62443 oder ISO 27001 bieten eine Schritt-für-Schritt-Anleitung, die für jedes Unternehmen und jede Situation gleichermaßen geeignet ist. Doch was sind die Gründe dafür, dass es keine einheitliche Vorgehensweise gibt? Folgende Punkte geben Antworten:

- ***Dynamische Bedrohungslandschaft***: Cyber-Bedrohungen entwickeln sich ständig weiter. Was heute als sicher gilt, kann morgen schon überholt sein.
- ***Individuelle Anforderungen***: Jedes Unternehmen hat andere Anforderungen, Strukturen und Risiken. Eine starre Vorgabe würde vielen Unternehmen nicht gerecht werden.
- ***Technologische Vielfalt***: IT-Landschaften sind heterogen und komplex. Eine Universallösung für alle Technologien und Systeme gibt es nicht.

Der Nutzen für Unternehmen

Diese Richtlinien und Normen dienen als Rahmen und definieren Grundprinzipien für ein solides Cybersicherheitsmanagement. Sie bieten aus praktischer Sicht:

- ***Bewährte Verfahren***: Bewährte Methoden und Verfahren, die in der Praxis erprobt und getestet wurden.
- ***Anforderungen***: Spezifische Anforderungen, die Unternehmen erfüllen sollten, um ein angemessenes Sicherheitsniveau zu erreichen.
- ***Strukturierung***: Sie helfen dabei, einen systematischen Ansatz zur Verbesserung der Cybersicherheit zu entwickeln.

Die Umsetzung liegt aber in den Händen der Unternehmen. Die eigentliche Herausforderung besteht darin, diese Rahmenbedingungen an die spezifischen Bedürfnisse des Unternehmens anzupassen und umzusetzen. Daher folgt an dieser Stelle ein Praxisleitfaden, den ich aufgrund meiner Erfahrung erstellt habe, natürlich ohne Anspruch auf Vollständigkeit.

Praktischer Leitfaden zur Umsetzung des CRA

Die Umsetzung des Cyber Resilience Act (CRA) und die Einhaltung von Normen wie IEC 62443 und ISO 27001 stellen Organisationen vor große Herausforderungen. Dieser Leitfaden soll Ihnen helfen, einen strukturierten Ansatz für die Umsetzung zu entwickeln.

1. Bestandsaufnahme und Risikoanalyse

- ***Erfassen Sie die IT-Landschaft***: Erstellen Sie eine detaillierte Bestandsaufnahme Ihrer IT-Systeme, Anwendungen und Daten.
- ***Identifizieren Sie geschäftskritische Prozesse***: Bestimmen Sie, welche Prozesse für Ihr Unternehmen am wichtigsten sind und welche Daten am sensibelsten sind.
- ***Bewerten Sie Risiken***: Führen Sie eine umfassende Risikobewertung durch, um potenzielle Bedrohungen und Schwachstellen zu ermitteln.
- ***Analysieren Sie die rechtlichen Anforderungen***: Prüfen Sie, welche spezifischen Anforderungen der CRA und anderer einschlägiger Gesetze für Ihr Unternehmen gelten.

2. Zielsetzung und Strategieentwicklung

- ***Definieren Sie Ziele***: Setzen Sie klare und messbare Ziele für Ihre Cybersicherheitsinitiativen.
- ***Entwickeln Sie eine Strategie***: Erstellen Sie auf der Grundlage Ihrer Risikoanalyse eine umfassende Cybersicherheitsstrategie, die Ihre Ziele unterstützt.
- ***Erstellen Sie einen Fahrplan***: Entwickeln Sie einen detaillierten Umsetzungsplan mit spezifischen Maßnahmen und Zeitplänen.

3. Umsetzung der Maßnahmen

- ***ISMS einführen***: Führen Sie ein Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 ein, um Ihre Informationssicherheit systematisch zu gewährleisten.
- ***Technische Maßnahmen***: Implementierung geeigneter technischer Maßnahmen wie Firewalls, Intrusion Detection Systeme, Verschlüsselung und Zugangskontrollen.
- ***Organisatorische Maßnahmen***: Führen Sie Mitarbeiterschulungen durch, legen Sie Prozesse für den Umgang mit Sicherheitsvorfällen fest und sensibilisieren Sie Ihre Lieferanten für das Thema Cybersicherheit.
- ***OT-Sicherheit***: Unternehmen mit industriellen Automatisierungssystemen sollten die Anforderungen der IEC 62443 umsetzen.

4. Kontinuierliche Verbesserung

- ***Überwachung und Bewertung***: Überwachen Sie kontinuierlich Ihre Sicherheitsmaßnahmen und führen Sie regelmäßige Bewertungen durch.
- ***Anpassen***: Passen Sie Ihre Sicherheitsmaßnahmen an neue Bedrohungen und technologische Entwicklungen an.
- ***Reaktion auf Vorfälle***: Entwickeln Sie einen wirksamen Plan zur Reaktion auf Vorfälle, um schnell und angemessen auf Sicherheitsvorfälle zu reagieren.

5. Unterstützung durch Beratung

- ***Externes Fachwissen***: Holen Sie sich externe Unterstützung von Cybersicherheitsexperten, um Ihre Projekte zu begleiten.
- ***Zertifizierung***: Ziehen Sie eine Zertifizierung nach ISO 27001 oder IEC 62443 in Betracht, um die Wirksamkeit Ihrer Maßnahmen nachzuweisen.

Fazit

In diesem zweiteiligen Artikel haben wir uns der Cybersicherheit mit einer Analogie aus dem Privatleben genähert und später den Blick auf die Bedeutung für die Industrie gelenkt. Durch die detaillierte Betrachtung der Normen ist klar geworden, dass Cybersicherheit für jedes Unternehmen individuell betrachtet werden muss und eine ganzheitliche Aufgabe darstellt.

Im Rahmen dieses Beitrags konnte nur ein Überblick verschafft werden, für eine Umsetzung in Ihrem Unternehmen empfehle ich Spezialisten zu konsultieren und eine maßgeschneiderte Lösung für den individuellen Fall zu finden.

FÜR SCHNELLLESER

Der zweite Teil des Beitrags befasst sich zunächst mit dem Cyber Resillience Act (CRA) im Allgemeinen und was dieser für Unternehmen bedeutet

Im weiteren Verlauf schildert der Autor das Zusammenspiel von CRA und den im ersten Teil besprochenen Normen IEC 62443 und ISO 27001

Abschließend wird dem Leser ein Leitfaden zur Umsetzung im eigenen Betrieb an die Hand gegeben

Autor:
Michael Wiener, M. Eng,
Dozent am Fachbereich Elektro- und Informationstechnik der Hochschule Fulda